COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

HIPAA Privacy Rule: Myths & Facts

Myth: Healthcare Providers Can Share Health Information With Employers

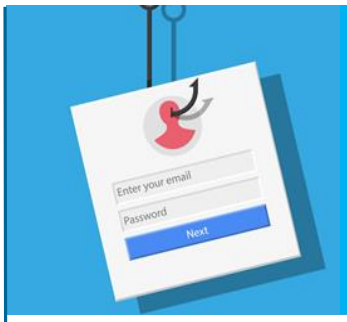
"Employers must have the ability to research health information about their current or potential employees. It's on the same level as information about their labor experience, education, skills, driving license, etc."

Fact: HIPAA prohibits healthcare providers from disclosing personal health information to employers without patient's consent.

In most cases, employers are not allowed to access a patient's medical records. This is not dependent on whether they are paying for their care or on their insurance plan.

The employer may obtain access to your medical records but only if you give your explicit, written permission. However, HIPAA does not cover healthcare information collected separately — for example, through HR surveys.

Resource:
https://www.qminder.com/hipaa-myths-debunked/



Fake VPN Alerts Used as Lure in Office 365 Credential Phishing Campaign

A phishing campaign has been identified that uses fake VPN alerts as a lure to get remote workers to divulge their Office 365 credentials.

Healthcare providers have increased their telehealth services during the COVID-19 public health emergency in an effort to help prevent the spread of COVID-19 and ensure that healthcare services can continue to be provided to patients who are self-isolating at home.

Virtual private networks (VPNs) are used to support telehealth services and provide secure access the network and patient data. Several vulnerabilities have been identified in VPNs which are being exploited by threat actors to gain access to corporate networks to steal sensitive data and deploy malware and ransomware. It is therefore essential for VPN systems to be patched promptly and for VPN clients on employee laptops to be updated. Employees may therefore be used to updating their VPN.

Researchers at Abnormal Security have identified a phishing campaign that impersonates a user's organization and claims there is a problem with the VPN configuration that must be addressed to allow the user to continue to use the VPN to access the network.

The emails appear to have been sent by the IT Support team and include a hyperlink that must be clicked to install the update. The user is told in the email that they will be required to supply their username and password to login to perform the update.

Read entire article:
https://www.hipaajournal.com/fake-vpn-alerts-used-as-lure-in-office-365-credential-phishing-campaign/

DID YOU KNOW...

Are Data Breaches HIPAA Violations?

Being HIPAA compliant is not about making sure that data breaches never happen. HIPAA compliance is about reducing risk to an appropriate and acceptable level. Just because an organization experiences a data breach, it does not mean the breach was the result of a HIPAA violation. The OCR breach portal now reflects this more clearly. Many data breaches are investigated by OCR and are found not to involve any violations of HIPAA Rules. Consequently, the investigations are closed without any action being taken.

Resource: https://www.hipaajournal.com/common-hipaa-violations/

MIDLAND HEALTH

NEWS

Bipartisan Bill Introduced to Protect Privacy of COVID-19 Contact Tracing and Exposure Notification Apps

A bipartisan group of Senators have introduced a bill that aims to regulate contact tracing and exposure notification apps that will be used to control the spread of COVID-19.

The Exposure Notification Privacy Act is one of three bills that aim to regulate contact tracing apps to protect the privacy of Americans. The other two bills failed to gather enough support. It is hoped a bipartisan bill will have a greater chance of being passed.

Contact tracing and exposure notification technologies are currently being explored as a way of controlling the spread of COVID-19. Google and Apple have both developed the technology to support contact tracing via mobile phones using low energy Bluetooth. When a user downloads a contact tracing app it will log encounters with other individuals who have also downloaded the app. When someone is diagnosed with COVID-19, the encounter data in the app is used to notify all individuals who may have been infected by that person.

Contact tracing and exposure notification apps have been used in other countries and have helped reduce the spread of COVID-19, but there are privacy risks associated with the apps that the new bill aims to address.

The Exposure Notification Privacy Act was introduced by Sens. Maria Cantwell (D-Washington) and Bill Cassidy (R-Louisiana) and has been co-sponsored by Amy Klobuchar (D-Minnesota). The bill aims to give Americans control over their personal data and "will place public health officials in the driving seat of exposure notification development."

The bill requires the use of contact tracing and exposure notification apps to be voluntary and for developers of the apps to implement measures that give consumers strong controls over their personal data. The bill limits the types of data that the apps can collect and places a time limit on how long personal data can be used.

Read entire article:
https://www.hipaajournal.com/bipartisan-bill-introduced-to-protect-privacy-of-covid-19-contact-tracing-and-exposure-notification-apps/

HIPAAQuiz

As a healthcare worker, you may share PHI for which of the following?

a. treatment
b. payment
c. healthcare operations
d. all of the above

Answer: d

Reason: HIPAA does not restrict healthcare workers from sharing PHI for treatment, payment, or healthcare operations. This includes using or disclosing PHI to properly care for a patient, ensure proper billing, and aid in quality-improvement efforts.

NEWS

Mobile Phishing Attacks Have Surged During the COVID-19 Health Crisis

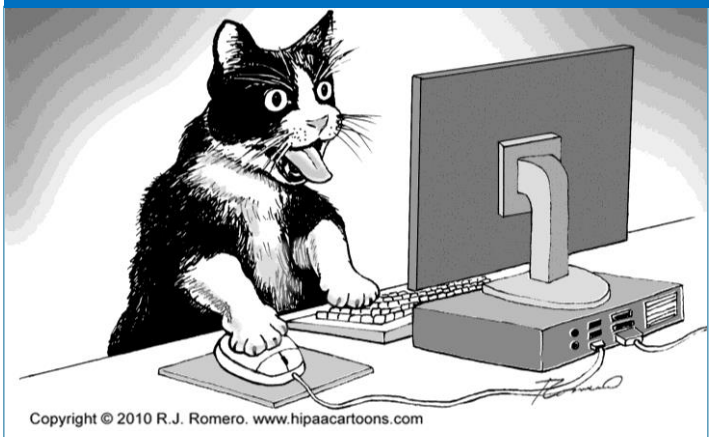
Cybercriminals have changed their tactics, techniques, and procedures during the COVID-19 health crisis and have been targeting remote workers using COVID-19 themed lures in their phishing campaigns. There has also been a sharp increase in the number of phishing attacks targeting users of mobile devices such as smartphones and tablets, according to a recent report from mobile security company Lookout.

Globally, mobile phishing attacks on corporate users increased by 37% from Q4, 2019 to the end of Q1, 2020 with an even bigger increase in North America, where mobile phishing attacks increased by 66.3%, according to data obtained from users of Lookout's mobile security software. Phishers have also been targeting remote workers in specific industry sectors such as healthcare and the financial services.

While the sharp increase in mobile phishing attacks has been attributed to the change in working practices due to the COVID-19 pandemic, there has been a steady rise in mobile phishing attacks over the past few quarters. Phishing attacks on mobile device users tend to have a higher success rate, as users are more likely to click links than when using a laptop or desktop as the phishing URLs are harder to identify as malicious on smaller screen sizes.

Read entire article:
https://www.hipaajournal.com/mobile-phishing-attacks-have-surged-during-the-covid-19-health-crisis/

HIPAA Humor



Copyright © 2010 R.J. Romero. www.hipaacartoons.com

Max was shocked and outraged to find cell phone photos of his recent neuter procedure posted on his veterinarian's FaceBook page.

IN OTHER COMPLIANCE NEWS

LINK 1

Aveanna Healthcare Facing Class Action Lawsuit Over 2019 Phishing Attack

https://www.hipaajournal.com/aveanna-healthcare-facing-class-action-lawsuit-over-2019-phishing-attack/

LINK 2

interlinkONE Confirmed as HIPAA Compliant by Compliancy Group

https://www.hipaajournal.com/interlinkone-confirmed-as-hipaa-compliant-by-compliancy-group/

LINK 3

HHS' OIG to Scrutinize HHS COVID-19 Response and Recovery Efforts

https://www.hipaajournal.com/hhs-oig-to-scrutinize-hhs-covid-19-response-and-recovery-efforts/

LINK 4

Kaiser Permanente Discovers 8-Year Employee HIPAA Breach

https://www.hipaajournal.com/kaiser-permanente-discovers-8-year-employee-hipaa-breach/

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing Awareness of HIPAA, PII, PHI, ePHI & Social Media

MIDLAND HEALTH

- ***Main Campus***
- ***West Campus***
- ***Legends Park***
- ***501a Locations***